VICTOR JIH, SBN 186515
vjih@wsgr.com
KELLY H. YIN, SBN 328380
kyin@wsgr.com
WILSON SONSINI GOODRICH & ROSATI, P.C.
1900 Avenue of The Stars, 28th Floor
Los Angeles, CA 90067
Telephone: (424) 446-6900
Facsimile: (866) 974-7329

LUIS LI, SBN 156081
luis.li@wsgr.com
WILSON SONSINI GOODRICH & ROSATI, P.C.
953 East Third Street, Suite 100
Los Angeles, CA 90071
Telephone: (323) 210-2900

SHERYL S. BASSIN, NY SBN 4662797
sbassin@wsgr.com
(admitted *pro hac vice*)
DYLAN G. SAVAGE, CA SBN 310452
dsavage@wsgr.com
WILSON SONSINI GOODRICH & ROSATI, P.C.
1301 Avenue of the Americas. 40th Floor
New York, NY 10019
Telephone: (212) 999-5800
Facsimile: (866) 974-7329

THOMAS WAKEFIELD, SBN 330121
twakefield@wsgr.com
WILSON SONSINI GOODRICH & ROSATI, P.C.
One Market Plaza, Spear Tower, Suite 3300
San Francisco, CA 94105
Telephone: (424) 446-6900

Attorneys for Defendants TikTok Inc. and ByteDance Inc.

UNITED STATES DISTRICT COURT

CENTRAL DISTRICT OF CALIFORNIA

BERNADINE GRIFFITH, et al., Individually and on behalf of all others similarly situated,

Plaintiffs,

v.

TIKTOK INC., a corporation; BYTEDANCE, INC. a corporation,

Defendants.

Case No. 5:23-cv-0964-SB-E

DEFENDANTS' REPLY IN SUPPORT OF DEFENDANTS' MOTION FOR SUMMARY JUDGMENT

REDACTED VERSION OF DOCUMENT PROPOSED TO BE FILED UNDER SEAL

Judge: Hon. Stanley Blumenfeld, Jr.
Date: November 1, 2024
Time: 8:30 a.m.
Place: Courtroom 6C

Action Filed: May 26, 2023
Trial Date: January 20, 2025

TABLE OF CONTENTS

TABLE OF AUTHORITIES

Page(s)

CASES

STATUTES

TABLE OF ABBREVIATIONS

Defendants	TikTok Inc. and ByteDance Inc.
EAPI	Events Application Programming Interface ("API")
Ex. __	Exhibit(s) attached to the Joint Appendix of Evidence, Dkt. 266-3 through 266-8
JB	Joint Brief re Defendants' Motion for Summary Judgment, Dkt. 269-1
Plaintiffs	Bernadine Griffith, Jacob Leady (Watters), and Patricia Shih
TikTok	The TikTok platform
TTI	TikTok Inc.

I. INTRODUCTION

The Joint Brief confirms that no evidence supports Plaintiffs' claims. Their theory relies on the disclosure of URLs they visit. Defendants pressed Plaintiffs to specify the URLs that were unlawfully disclosed. After 18 months of litigation, they identify [redacted]. None are actionable. [redacted].

Plaintiffs' evidence shows only that some of Plaintiffs' browsing history was shared with TikTok. But, absent special circumstances that do not exist here, data sharing does not violate Plaintiffs' rights. For the Internet to work, such information must be shared. Indeed, the terms that Plaintiffs agreed to expressly disclose that websites share information with third parties like Defendants. Given the lack of special circumstances or offensive disclosures, Plaintiffs' claims fail.

II. ARGUMENT

A. Plaintiffs' Attempt to Expand the Claims Beyond the Six Websites Identified in the Complaint Should Be Rejected.

Plaintiffs reprimand Defendants for saying this case concerns the "six websites" identified in the Complaint when it should really be about "tens of thousands of websites." JB 2. Yet Plaintiffs refused discovery into their browsing history beyond these six websites until after summary judgment was filed.

Plaintiffs cannot rely on evidence they refused to produce. When Defendants asked for Plaintiffs' browsing history over a year ago, Plaintiffs refused and only provided discovery for the six websites. *See* Ex. 29 ¶¶ 80-87 (analyzing limited browsing data); Dkt. 264-1 at 35 n.8. Now that it is clear they can identify only [redacted]

[redacted], Plaintiffs improperly attempt to change course. After Defendants filed this motion, and at the close of discovery, they produced their history.

Plaintiffs cannot gain an advantage by taking inconsistent positions throughout this litigation. *Cf. Hamilton v. State Farm Fire & Cas. Co.*, 270 F.3d 778, 783 (9th Cir. 2001) (party cannot take "inconsistent positions in the same litigation"). Having argued that their browsing data is irrelevant and not made it available as evidence on summary judgment, they cannot now claim the opposite. *See Rago v. Select Comfort Retail Corp.*, 2020 WL 8611033, at *6 (C.D. Cal. Dec. 9, 2020) (plaintiff cannot rely on evidence produced after summary judgment stipulation is served).

B. The 24 URLs Plaintiffs Identify From Their Browsing History Do Not Show a Violation of Plaintiffs' Privacy Rights.

Plaintiffs identify 24 disclosures that they believe support their privacy claims.[1] JB 13-16. None do.

First, there is no evidence the 24 URLs were disclosed to TTI; Plaintiffs assume this happened. Plaintiffs' expert [redacted]. Ex. 57 ¶ 64. This is insufficient. Plaintiffs do not say, via declaration or otherwise, [redacted]. Even then, Plaintiffs use tools that could block such disclosures. JAF-18-21. They cannot assume, without evidence, that every URL was disclosed. *See AV Media Pte. Ltd. v. Promounts*, 2008 WL 11337209, at *3 (C.D. Cal. July 1, 2008) ("[T]he summary judgment stage [is] the 'put up or shut up' moment in a lawsuit, when the nonmoving party must show what evidence it has.").

Second, the 24 URLs do not identify Plaintiffs. The disclosure of anonymous browsing data does not violate privacy rights. *Cahen v. Toyota Motor*

[1] Six for Griffith, thirteen for Shih, and five for Watters. JB 14-15.

Corp., 717 F. App'x 720, 724 (9th Cir. 2017) (no claim for "non-individually identifiable" information); *Byars v. Sterling Jewelers, Inc.*, 2023 WL 2996686, at *3 (C.D. Cal. Apr. 5, 2023) (no claim when no "specific personal information" was disclosed); *Lightoller v. JetBlue Airways Corp.*, 2023 WL 3963823, at *4 (S.D. Cal. June 12, 2023) (no claim for anonymized activity); *I.C. v. Zynga, Inc.*, 600 F. Supp. 3d 1034, 1049 (N.D. Cal. 2022) (no claim when "anonymity is preserved"); *Massie v. GM LLC*, 2022 WL 534468, at *5 (D. Del. Feb. 17, 2022) (no "reasonable expectation of privacy over the anonymized data").

Plaintiffs argue that the data sent with the URLs could be identifying. JB 11-18. But Plaintiffs cannot speculate—they must show Defendants can "identify or extract" specific data. Dkt. 283 at 4 n.2. They do not. [redacted][2] Dkt. 297-2 ¶ 43.[3]

Third, these URLs do not disclose any "sensitive information." *In re Facebook, Inc. Internet Tracking Litig.*, 956 F.3d 589, 605 (9th Cir. 2020). URLs that "reveal[] only basic identification and address information" are not sensitive or private. *Hammerling v. Google LLC*, 615 F. Supp. 3d 1069, 1089 (N.D. Cal. 2022). A URL for a product is not sensitive or private because it would be no

[2] Plaintiffs argue that hashed emails and phone numbers can be identifying, but that is true only if Defendants already know that information. Dkt. 283 at 4 n.2. Defendants do not have this information for non-TikTok users. Plaintiffs offer no evidence otherwise, or that TikTok engaged the services that could contain Plaintiffs' information, or that Defendants tried to identify non-TikTok users. Instead, Defendants discard such data. *Id.* at 1.

[3] Dr. Shafiq's rebuttal report does nothing to help Plaintiffs' arguments. In any event, the report is improper because it includes new arguments and evidence.

different from browsing in a "brick-and-mortar store." *Cook v. GameStop, Inc.*, 689 F. Supp. 3d 58, 66 (W.D. Pa. 2023). Neither is looking at a URL containing "general health information." *Smith v. Facebook, Inc.*, 262 F. Supp. 3d 943, 955 (N.D. Cal. 2017) (HIPAA claims).

[redacted].

The law simply does not prohibit "the disclosure of common, basic digital information to third parties." *In re Google, Inc. Privacy Policy Litig.*, 58 F. Supp. 3d 968, 985 (N.D. Cal. 2014). The collection of browsing data is not outside a reasonable person's "common-sense expectation." *Hammerling*, 615 F. Supp. 3d at 1089. This is not a case where a company says that it will not collect data and then does. *See Brown v. Google LLC*, 685 F. Supp. 3d 909, 924 (N.D. Cal. 2023) (Incognito browsing mode); *Facebook Tracking*, 965 F.3d at 605 (logged out users). Nor is this a case where disclosures go beyond identifying information and reveal the person's health or their finances.

C. The Three URLs Plaintiffs Identify Do Not Show That Any Contents of Plaintiffs' Communications Were Intercepted.

1. The URLs Do Not Contain the Contents of Communications.

Plaintiffs identify [redacted].[4] JB 22-23. None of these contains the "contents" of Plaintiffs' communications. A URL that shows just the "particular document within a website that a person views" does not reveal any "contents." *In re Zynga Privacy Litig.*, 750 F.3d 1098, 1108 (9th Cir. 2014). The URL must show what Plaintiffs said to or on the webpage, like the "search queries" sent or information a visitor provides. *Brown*, 685 F. Supp. 3d at 935. [redacted]. JB 22.

Plaintiffs also cannot rely on mouse movements, keystrokes, and button clicks. JB 23-24. Plaintiffs have no evidence that their metadata was collected. Regardless, metadata is not "contents." *See Cook*, 689 F. Supp. 3d at 70.

2. No Communications Were Intercepted "in Transit."

This is a rare instance where the experts on both sides agree. Plaintiffs' expert agrees that [redacted]. JB 20-21. [redacted]. *Id.* [redacted]. *Id.* 21. These tools do not "intercept" the user's communication with a website "during transmission." *Konop v. Hawaiian Airlines, Inc.*, 302 F.3d 868, 878 (9th Cir. 2002).

[4] Plaintiffs argued wiretapping for two additional URLs. JB 22-23. [redacted]. Dkt. 297-2 ¶ 43.

This case is like *Gonzales v. Uber Techs., Inc.*, 305 F. Supp. 3d 1078 (N.D. Cal. 2018). There, the plaintiff alleged Uber sent fake rider requests to Lyft to obtain Lyft driver information. *Id.* at 1083. A Lyft driver argued that Uber intercepted his communications with Lyft. *Id.* at 1084. The court disagreed. "[T]he communication Uber acquired is a communication from Lyft and not Plaintiff and therefore Lyft did not intercept Plaintiff's communications." *Id.* at 1086. The same is true here.

Plaintiffs' focus on how soon the disclosure takes place is irrelevant, JB 23-24, because the law turns not on speed but on the sequence of events. *See Konop*, 302 F.3d at 878. Interception is concerned with acquiring contents while they are still in transit; there is no interception if contents are disclosed after receipt. *See Flanagan v. Flanagan*, 27 Cal. 4th 766, 775-76 (2002). [redacted] JB 25. [redacted]. Plaintiffs do not dispute that [redacted].[5]

Plaintiffs find no support in *United States v. Szymuskiewicz*, 622 F.3d 701 (7th Cir. 2010). There, an employee who configured his boss's computer to forward all emails to him was liable for interception because they were forwarded before the boss opened them. *Id.* at 702-03. Here, [redacted]

[5] Plaintiffs never address Defendants' argument that the creator of a tool is not liable for another person's use of "technology created by others." JB 21. Their failure to respond is a concession. *See, e.g., Robison v. Amcal Wood Ranch Fund XXXVII*, 2008 WL 9888773, at *15 (C.D. Cal. Sept. 23, 2008). Plaintiffs provide no evidence that Defendants have specific knowledge of, contribute to, control, or induce any wiretapping by advertisers.

[redacted] JB 21-22.

Nor does *Gruber v. Yelp Inc.*, 55 Cal. App. 5th 591, 607 (2020), support Plaintiffs' argument because that case concerned *recording*, not *interception*. Plaintiffs conflate these different actions even though they are governed by separate provisions. Section 632(a) prohibits the recording of any part of a conversation without consent. Cal. Penal Code § 632(a). Section 631(a), on which Plaintiffs base their claim, prohibits the taking of a communication while it is "in transit"; *i.e.*, when or after it is sent, but before it is received. *Konop*, 302 F.3d at 878; Cal. Penal Code § 631(a). Plaintiffs cannot save their interception claims with precedent about recordings.

D. Plaintiffs Consented to Sharing Their Online Activity With Partners Like TikTok.

1. Plaintiffs Expressly Consented by Agreeing to Each Website's Privacy Policies.

It is undisputed that the six named websites have policies containing broad language disclosing that they send visitors' browsing information to third parties, including through the use of pixels or other similar technologies. JAF-48-49, 52-54, 58-62, 65-76. A reasonable person would understand these broad disclosures to include TikTok's Pixel and EAPI. *See Calhoun v. Google, LLC*, 113 F.4th 1141, 1147 (9th Cir. 2024) (objective standard).

Plaintiffs argue there is no express consent because these policies do not specifically mention Defendants. JB 34-35. Plaintiffs cite no authority for this. Nor does it make sense. In Plaintiffs' world, it would be impossible to agree that information can be disclosed to "any person" simply because every person is not named. *F.B.T. Prods., LLC v. Aftermath Records*, 621 F.3d 958, 964 (9th Cir. 2010) (a term is not unenforceable "just because it is broad"). If Plaintiffs were

right, many consent cases based on similarly non-specific disclosures would be implicitly overruled. *See Smith*, 262 F. Supp. 3d at 954 ("third-party websites"); *Mortensen v. Bresnan Commc'n, L.L.C.*, 2010 WL 5140454, at *3 (D. Mont. Dec. 13, 2010) ("third parties that provide content or services"); *Perkins v. LinkedIn Corp.*, 53 F. Supp. 3d 1190, 1197 (N.D. Cal. 2014) ("some information").

Plaintiffs' cases are inapplicable because the policies *misrepresented* the practices. *See Brown*, 685 F. Supp. 3d at 928 (Incognito Mode said it would not collect data); *Opperman v. Path, Inc.*, 205 F. Supp. 3d 1064, 1072-74 (N.D. Cal. 2016) (policies stated data would be "access[ed]," not "upload[ed]"); *Calhoun*, 113 F.4th at 1150-51 (Google stated it would not sync data). These cases do not require specificity—just truthfulness.

Finally, Plaintiffs claim "law-of-the-case" forecloses consent because the Court denied Defendants' motion to dismiss. JB 33. Nonsense. *See Askins v. U.S. Dep't of Homeland Sec.*, 899 F.3d 1035, 1042 (9th Cir. 2018). More importantly, the Court merely declined to decide consent before discovery. The Court never said broad disclosures are defective, nor did it rule on the sufficiency of the disclosures. Now that the facts are developed, they show Plaintiffs consented.

2. Plaintiffs' Continued Browsing of These Websites Shows Implicit Consent to the Data Transfer.

Most of Plaintiffs' website visits occurred after they joined this lawsuit, when they understood that TikTok's tools were collecting their information. In fact, only 22 out of 544 visits came before the lawsuit. Exs. 11-12, 21-27.[6]

The post-lawsuit visits are not actionable. Plaintiffs cannot manufacture claims by going back to the same websites repeatedly with full knowledge of the

[6] This is not surprising because Plaintiffs clear their browsing history. Dkt. 264-1 at 35 n.8. There is no reason to believe that Plaintiffs' last-minute production of their entire browsing history is different. Indeed, that [redacted].

collection. JB 32. To the contrary, their visits knowing their information is being collected shows implied consent and proves that they have no actual objection to what the websites shared with Defendants. *Id.*

Plaintiffs' only response is to say it would be unfair to make them stop visiting these websites. JB 39-40. It is not unfair—there is no law prohibiting the consensual collection of data. Plaintiffs can continue browsing; they simply cannot visit the sites knowing of the data collection and pretend they were injured. Put otherwise, Plaintiffs cannot complain of an alleged harm when they intentionally subject themselves to it. *See, e.g.*, *Berni v. Barilla S.P.A.*, 964 F.3d 141, 148-49 (2d Cir. 2020) (knowledge of deceptive advertising precluded forward-looking relief).

Their cases do not say otherwise. In *Rodriguez v. Google LLC*, even if individuals chose to deny access to their data on the front end, Google allegedly collected the data anyway; their continued use of Google's services does not mean they consented to the deception. 2024 WL 38302, at *1 (N.D. Cal. Jan. 3, 2024). The plaintiffs in *In re Yahoo Mail Litigation* were not Yahoo mail users and could not possibly consent to Yahoo's practices. 308 F.R.D. 577, 589 (N.D. Cal. 2015).

E. Plaintiffs Have No Evidence That There is a Market for of Any Financial Value in Five or Six URLs Each.

As this Court has held, property claims require proof that there is a market for the data or that it has financial value. Dkt. 242 at 11. The evidence here shows that Defendants' tools are used on "a relatively small percentage of websites." *Id.* In fact, Plaintiffs identify just a few URLs each.

Plaintiffs offer no evidence of any market for such incomplete data. The only evidence Plaintiffs have is for very different data. JB 43-44. Screenwise and SavvyConnect pay only for far more systematic and complete access to a person's

browsing activity over long periods of time. Dkt. 195-18 ¶¶ 54-55. There is no market for haphazard and sparse browsing histories.

III. CONCLUSION

Plaintiffs' attempt to build their case on browsing histories they refused to produce until recently, even if permitted, fails as well. There is no evidence that any URL disclosed to TTI invaded any privacy interest, entailed any interception of communications, or impaired any property interest. Plaintiffs have no basis to complain when they agreed to the websites' data disclosures, and they continued to visit them even after filing this lawsuit. With no evidence to support them, Plaintiffs' claims fail.

Defendants respectfully request that the Court enter summary judgment in their favor.

Dated: October 18, 2024

WILSON SONSINI GOODRICH & ROSATI
Professional Corporation

By: */s/ Victor Jih*
Victor Jih

Attorney for Defendants
TikTok Inc. and ByteDance Inc.

CERTIFICATE OF COMPLIANCE

The undersigned, counsel of record for Defendants TikTok Inc. and ByteDance Inc., certifies that this brief contains 2,996 words, which complies with the word limit of this Court's Order re Motions for Summary Judgment ¶ 2(f).

Dated: October 18, 2024

WILSON SONSINI GOODRICH & ROSATI
Professional Corporation

By: */s/ Victor Jih*
Victor Jih

Attorney for Defendants
TikTok Inc. and ByteDance Inc.